

INFORMATION SECURITY POLICY

POLICY NUMBER:
ISM 8

SUBJECT:

RISK ASSESSMENT AND TREATMENT POLICY

DISTRIBUTION DATE:
6/1/2014

EFFECTIVE DATE:
6/1/2014

ISSUING AUTHORITY: Director of Information Technology Services of the
Metropolitan Government of Nashville and Davidson County

EXPIRATION: UNTIL
RESCINDED

PURPOSE

The purpose of this Policy is to ensure that the Metropolitan Government of Nashville and Davidson County (Metropolitan Government) properly inventories and manages its assets, and undertakes a risk assessment and treats identified risks.

POLICY

1. Comprehensive Risk Management Strategy

Metropolitan Government shall:

- a) Develop a comprehensive strategy to manage risk to its operations and assets, individuals, other organizations, and the city associated with the operation and use of information systems; and
- b) Implement that strategy consistently across its departments, agencies and boards.

2. Risk Management Process

The Metropolitan Government information security risk management process shall consist of: (i) context establishment; (ii) risk assessment; (iii) risk treatment; (iv) risk monitoring and review. Metropolitan Government shall assess risk to operations, assets and individuals from operation of information systems and associated processing, storage or transmission of information.

Metropolitan Government shall utilize appropriate industry-accepted standards, frameworks and guidance for its risk assessment and treatment program such as:

- ISO/IEC 27002 Code of Practice for information Security Management;
- ISO/IEC 27005 Information Security Risk Management;
- NIST SP 800-39 Managing Risk from Information Systems: An Organizational Perspective;
- NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach; and
- NIST SP 800-30 Risk Management Guide for Information Technology Systems.



3. Context Establishment

- a. Define Scope of Risk Assessment
- b. Information Classification and and Asset Categorization - Within the scope defined above, the Metropolitan Government shall:
 1. Classify and categorize information and the information system as described in the Information Classification Policy and the Inventory of Assets Policy.
 2. Document the classification/categorization results (including supporting rationale) in the security plan for the information system; and
 3. Ensure the classification/categorization decision is reviewed and approved by the director, head or chair of each Metropolitan Government department, agency or board.

4. Risk Assessment

Metropolitan Government shall:

- a. Undertake a risk assessment that identifies, quantifies the likelihood and magnitude of harm, and prioritizes risks against criteria for risk acceptance and objectives relevant to Metropolitan Government; and
- b. Document risk assessment results in a security plan.

5. Risk Treatment

Metropolitan Government shall:

- a. Develop a comprehensive strategy to treat identified risks by: (i) applying appropriate controls to reduce the risks; (ii) knowingly and objectively accepting risks; (iii) avoiding risks by not allowing the actions that would cause the risks to occur; and (iv) transferring the associated risks to third parties.
- b. Monitor, evaluate, and improve the efficiency of security controls.

6. Risk Monitoring and Review

The directors, heads, and chairs of its departments, agencies and boards shall monitor, review and update the efficiency and effectiveness of security controls. At minimum, a group review shall occur at least biannually, and these efforts will include, but are not limited to:

- a. Review effectiveness of risk assessment and treatment; and
- b. Update the risk assessment and treatment as set forth in the risk assessment activities procedures [risk assessment and treatment procedures] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.



SCOPE, BACKGROUND and GOVERNANCE

This information is set forth in the *Metropolitan Government Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Terms used in this policy are defined in the *Metropolitan Government Information Security Glossary*.

CONTACT

Questions should be directed to (615) 862-6222 or by email at ciso@nashville.gov, or by mailing them to CISO, Information Technology Services Department, 700 2nd Avenue South, Suite 301, P. O. Box 196300, Nashville, TN 37219-6300

SIGNATURE



Keith Durbin,
Chief Information Officer/Director of ITS
Metropolitan Government of Nashville and Davidson County

REFERENCES

- ISO 27002: section 4
- ISO 27005 Clause 6
- NIST Special Publication 800-53 Rev3, *Recommended Security Controls for Federal Information Systems and Organizations*: RA-1, RA-2, RA-3, RA-4
- FIPS 200 Risk Assessment (RA) Minimum Security Requirements

REVISION HISTORY

REVISION	APPROVAL DATE	CHANGES
1.0	7/1/2011	First released version
2.0	6/1/2014	Amended

